

# UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

INFORMATION ASSOCIATED WITH  
KEYSTONEINC11@GMAIL.COM THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE LLC

Case No. **1:20-MJ-00367**

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. 1028(a)(7), 1028A, 1343	Unlawful transfer, possession, or use of a means of identification; aggravated identity theft; and wire fraud, respectively

The application is based on these facts:

See attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



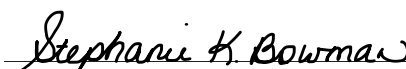
Applicant's signature

Sean Williams, Special Agent - TIGTA

Printed name and title

Sworn to before me and signed in my presence via electronic means.

Date: **May 20, 2020**



Judge's signature

City and state: Cincinnati, OH

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with:

- KEYSTONEINC11@GMAIL.COM

that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under Title 18 U.S.C. §2703(f) on April 30, 2020, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A (each an “Account”):

1. The contents of all emails and instant message communications associated with the Account from **July 1, 2011, through the present**, including stored or preserved copies of emails sent to and from the Account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

2. All records or other information regarding the identification of the Account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the Account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number) (collectively, “Account Identification Information”);

3. Source and destination addresses and header or routing information for each communication (including originating IP addresses of emails); the date, size, and length of each

communication; and any user or device identifiers linked to each communication (including cookies);

4. All records or other information stored by an individual using the Account, including address books, contact and buddy lists, calendar data, pictures, and files;

5. All device or user identifiers that have ever been linked to the Account, including but not limited to all cookies and similar technologies, unique application numbers, hardware models, operating system versions, device serial numbers, Global Unique Identifiers (“GUID”), mobile network information, telephone numbers, Media Access Control (“MAC”) addresses, and International Mobile Equipment Identities (“IMEI”);

6. All Account Identification Information (as defined above) for any accounts linked to the Account by a common email address (such as a common recovery email address), common telephone number, common means of payment (e.g., credit card number), common registration or login IP addresses (during a one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

7. The types of service utilized;

8. All records and other information concerning any record, document, or other computer file created, stored, revised, or accessed in connection with the account or by an account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers; and

9. All records pertaining to communications between the Provider and any person regarding the Account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the Special Agent listed below via United States mail, courier, or email within **14 days** of the issuance of this warrant:

Special Agent Sean Williams  
Sean.williams@tigta.treas.gov  
550 Main Street Room 5-610  
Cincinnati, OH 45202

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 1028(a)(7) (unlawful transfer, possession, or use of a means of identification), 1028A (aggravated identity theft), and 1343 (wire fraud), as well as conspiracy to commit the foregoing offenses, those violations involving VICTOR TORRES, ADESH BISSOON, MICHAEL JOSEPH, and other unknown persons and occurring during and after July 2011, specifically, for each account or identifier listed on Attachment A (each an “Account,” and collectively “the Accounts”), information pertaining to the following matters:

1. Information relating to the identification or location of the user(s) of the Account;
2. Information relating to persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) in the commission of the criminal activity under investigation; or (ii) communicated with the account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
3. Information relating to the Account user’s state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning related to the criminal activity under investigation;
4. Information relating to how and when the Account was accessed or used, to the geographic and chronological context of account access, use, and events relating to the crime under investigation and the account user;

5. Information relating to the theft and trafficking of personally identifiable information (PII);
6. Information relating to the identities of victims of identity theft;
7. Information relating to the use of stolen PII to commit other offenses, including but not limited to stealing or fraudulently obtaining funds through wire fraud or by filing fraudulent tax returns;
8. The identity of the person(s) who communicated with the Account about matters relating to the fraudulent scheme involving stolen PII, including records that help reveal their whereabouts;
9. All information pertaining to access to any Internal Revenue Service (“IRS”) website or service and any information obtained from the IRS or other tax-related information;
10. Evidence relating to the preparation or planning related to the criminal activities under investigation;
11. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
KEYSTONEINC11@GMAIL.COM THAT  
IS STORED AT PREMISES  
CONTROLLED BY GOOGLE LLC

Case No. **1:20-MJ-00367**

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Sean Williams, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with KEYSTONEINC11@GMAIL.COM (“the **Subject Account**”) that is stored at premises owned, maintained, controlled, or operated by Google LLC (“Google”), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Treasury Inspector General for Tax Administration (“TIGTA”) and have been since February 2018. Prior to my employment with TIGTA, I was a Special Agent, Investigator, and Police Officer with multiple government agencies. I am a graduate of the Criminal Investigator Training Program at the



Federal Law Enforcement Training Center in 2018. I am currently assigned to TIGTA's Mid Atlantic Field Division in the Cincinnati Office. I am also a member of the TIGTA Cyber Investigative Cadre (CIC). As a member of the CIC, I have received training from the National Cyber-Forensics and Training Alliance to be better equipped to investigate cases involving Cyber Crimes. I have also received specialized training in online research and have access to programs and databases designed to assist in Cyber investigations. I have investigated matters involving bank and wire fraud, impersonation fraud, theft of government monies, loss of IRS property and equipment, and threats and assaults towards the IRS and its employees. Throughout my training and experience with these types of investigations, I have encountered countless situations where email, the internet, and technical matters have been employed to conduct criminal activity. The Internet and email are the primary vehicles used by criminals to conduct these types of crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028(a)(7) (unlawful transfer, possession, or use of a means of identification), 1028A (aggravated identity theft), 1343 (wire fraud), and conspiracy to commit the foregoing violations (collectively, the "Target Offenses") have been committed. There is also probable cause to search the information described in Attachment A for the evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

**A. The government is investigating a suspected identity-theft scheme in which multiple subjects have exchanged stolen PII and fraudulent documents by email.**

6. The U.S. Attorney’s Office for the Southern District of Ohio and TIGTA are investigating a suspected identity-theft scheme in which victims’ stolen Personally Identifiable Information (PII) is being shared among multiple subjects via email. Some of the victims whose PII has been shared live in the Southern District of Ohio.

7. The investigation to date has identified at least three co-conspirators involved with the scheme: VICTOR TORRES, MICHAEL JOSEPH, and ADESH BISSOON. Search warrants have shown that TORRES, JOSEPH, and BISSOON have each used email accounts to send and receive PII belonging to many individuals.

8. For reasons given below, I believe that the **Subject Account** is one of the email accounts that MICHAEL JOSEPH has used in furtherance of this scheme.

**B. The Subject Account was exchanging stolen PII, fraudulent identification and documents, and suspected stolen credit card and bank account numbers with VTORR007@FIU.EDU as early as July 2011.**

9. In October 2019, I reviewed search warrant return data for VTORR007@FIU.EDU, an account that belongs to VICTOR TORRES. The return data went through September 2019.

10. In reviewing the results of the search warrant, I found that, as early as July 2011, the **Subject Account** was sending emails to VTORR007@FIU.EDU that contained many individuals' PII. The **Subject Account** and VTORR007@FIU.EDU continued to share PII, fraudulent Social Security cards, and fraudulent driver's licenses of victims through December 2014.

11. In my training and experience, the types of information being sent back and forth between the **Subject Account** and VTORR007@FIU.EDU—PII, fraudulent Social Security cards, fraudulent driver's licenses, and other fraudulent documents—is consistent with the trafficking of stolen identities. Parallel investigations by TIGTA have shown that these types of materials have been used to open bank accounts and credit cards, and to apply for loans, without authorization.

**C. The Subject Account was exchanging fraudulent documents with ABISSOON26@GMAIL.COM as recently as December 2019.**

12. In April 2020, I reviewed search warrant return data for another email address associated with the identity-theft scheme under investigation: ABISSOON26@GMAIL.COM. Based on the email signature for ABISSOON26@GMAIL.COM, which lists "Adesh Bissoon," I believe that ADESH BISSOON uses this email account.

13. The return data went through January 2020 and showed that, starting in at least November 2013 and continuing through approximately December 2019, ABISSOON26@GMAIL.COM sent to the **Subject Account**, and received from the **Subject Account**, emails containing PII belonging to many individuals, fraudulent Social Security cards, fraudulent driver's licenses, and fraudulent employment-verification letters.

14. For example, on September 9, 2016, the **Subject Account** sent a message to ABISSOON26@GMAIL.COM that contained the name, address, telephone number, last four digits of an SSN, company name, Employer Identification number (EIN), and income of P.J.<sup>1</sup> In this email, the user of the **Subject Account** wrote to ABISSOON26@GMAIL.COM: “[V]ouch for me in the event some lenders contact you sometimes next week...I’ve been with your company since 8-06-2013.” Based on my training and experience, I believe that the user of the **Subject Account** was asking BISSOON to provide P.J.’s PII to a lender in the event that the lender called to verify information that the user of the **Subject Account** had provided in connection with a loan or other financial account he had opened in P.J.’s name.

15. As another example, on December 17, 2019, the **Subject Account** (which uses the display name “Joseph”) sent a message to ABISSOON26@GMAIL.COM that said: “Hey bro here is attached the letter I just wrote.” Attached to the email was a letter that purported to be from “Gary Zets,” a manager at Engineering Acoustics, Inc.<sup>2</sup>

16. The letter’s memo line said “RE: Michael J. Joseph” (i.e., the full name of MICHAEL JOSEPH), and the letter stated in part: “I highly recommend Mr. Joseph to prospective leasing agents or property owners . . . [He] would be a tremendous addition to

---

<sup>1</sup> Based on my review of emails from accounts associated with MICHAEL JOSEPH, another known conspirator in this identity-theft scheme, I know that MICHAEL JOSEPH has previously used P.J.’s identity in furtherance of the crimes under investigation.

<sup>2</sup> According to [www.eaiinfo.com](http://www.eaiinfo.com), Engineering Acoustics, Inc. is a technology company that develops human-centric vibrotactile and haptic systems for defense, entertainment, simulation, and training. The website lists Gary Zets as the company’s CEO and President.

your community and has my highest recommendation.” The letter listed Gary Zets’s phone number as 512-XXX-XXXX and his email as zets.acoustics2@gmail.com.<sup>3</sup>

17. In the body of the email, the user of the **Subject Account** wrote to BISSOON:

Memo: I have been working for your company since march 3rd, 2014. I currently make about 60K annually before taxes. Every 2 weeks, I earn about 2300-2500 before taxes. My last pay-dates were on Friday December 13th, November 29th and November 15th. I get "direct Deposit". My status is single and Exemptions/Allowances is 0. My address on file is [redacted], Boynton Beach, FL 33426-8607

Please bro I am begging you to stay close to that 512# and keep it connected until i get approved even if I've to pay for it. I don't know how thorough those peeps are about their due-diligence and that's why i am taking all the necessary measures or precautions [....]

Regards,  
MJJ

18. Based on the fact that the display name associated with the **Subject Account** is “Joseph,” the fact that the user of the **Subject Account** signed this email with “MMJ” (MICHAEL JOSEPH’s initials), and the fact that the reference letter attached to the email was for “Michael J. Joseph,” I believe that JOSEPH is the user of the **Subject Account**.

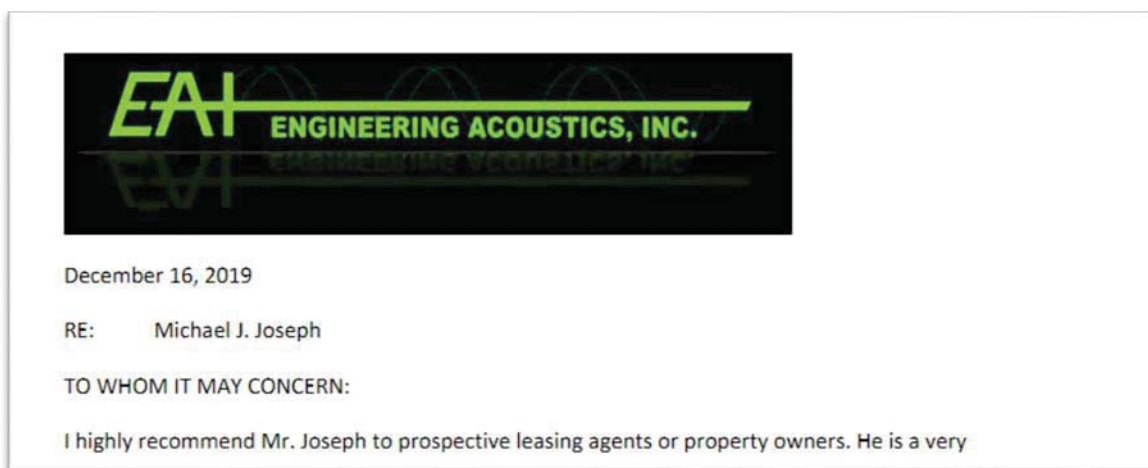
19. Based on my training and experience and knowledge of this case, I further believe that, in this email, JOSEPH was instructing BISSOON to pretend to be Gary Zets and to provide false information about JOSEPH’s alleged employment so that JOSEPH

---

<sup>3</sup> All email addresses listed on the “Contact Us” page for Zets Acoustics are at the domain @eaiinfo.com; there are no Gmail addresses. See “Contact Us,” *Engineering Acoustics Inc.*, available at <https://www.eaiinfo.com/contact/> (last accessed May 19, 2020).

could be approved for some type of application. When JOSEPH wrote, “I am begging you to stay close to that 512# and keep it connected until I get approved,” I believe he meant that BISSOON should answer the 512-XXX-XXXX phone number that JOSEPH had included on the fraudulent reference letter purporting to be from Gary Zets.

20. Later on December 17, 2019, BISSOON wrote back to the **Subject Account**: “see attached.” Attached to the email was a version of the recommendation letter purporting to be from Gary Zets. This version of the recommendation letter included the logo for Engineering Acoustics:



21. Based on my training and experience and knowledge of this case, I believe that in this email BISSOON was returning a revised copy of the fraudulent reference letter to JOSEPH so that JOSEPH could provide it to the third party from which JOSEPH was seeking approval of an application.

**D. In January 2020, agents executed a search warrant at TORRES's residence and found evidence that the scheme was ongoing.**

22. In January 2020, agents executed a search warrant at the home of one of the coconspirators, VICTOR TORRES, in Florida.

23. During the search, agents seized TORRES's phone, which contained many texts between TORRES and someone listed in the phone as "MIKE" that I believe were about identity theft. For example, on January 30, 2017, "MIKE" texted TORRES: "Hey bro could u please make a SSN for this guy for me? [Name redacted; SSN redacted]? I'll also email you his signature to fiukid...." And on June 23, 2017, "MIKE" texted TORRES: "Would u be able to please do one DL & SS for me???" Based on my training and experience, I believe that in these texts "MIKE" was asking TORRES to create fraudulent Social Security cards ("SSNs") and driver's licenses ("DLs") using stolen PII.

24. I believe that "MIKE" is MICHAEL JOSEPH, because the profile picture for "MIKE" appears to match MICHAEL JOSEPH's driver's license photo.

25. While searching TORRES's house, agents also discovered fraudulent credit cards, checks, driver's licenses, and other fraudulent documentation. I believe based on this evidence that TORRES and his coconspirators were still engaged in identity theft as of January 2020.

**E. Google likely has relevant evidence relating to the Subject Account.**

26. In my training and experience, individuals engaged in identity theft tend to follow the same modus operandi: The individuals fraudulently obtain PII, access the IRS's eAuthentication system to verify that the PII is valid, and then open fraudulent accounts in the names of the victims. The individuals then make online purchases, take out loans, and transfer money between accounts. In my training and experience, the contents of, and other records relating to, the email accounts used to traffic stolen PII provide a broader picture of the crime and help law enforcement identify the suspects.

27. On April 30, 2020, I sent a preservation request to Google to request that they preserve records associated with the **Subject Account**. Based on my training and experience, I know that, in general, an email that is sent to a Gmail subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

### **BACKGROUND CONCERNING EMAIL AND GOOGLE**

28. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in



address books, contact or buddy lists, email in the account, and attachments, including pictures and files.

30. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

31. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

32. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use

relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

### **CONCLUSION**

34. Based on the foregoing, I request that the Court issue the proposed search warrant.

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

### **REQUEST FOR SEALING**

36. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to

flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

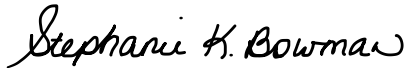
Respectfully submitted,



---

SEAN WILLIAMS  
Special Agent  
Department of the Treasury (TIGTA)

Subscribed and sworn to before me on May 20, 2020. **via electronic means.**



---

HON. STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with:

- KEYSTONEINC11@GMAIL.COM

that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under Title 18 U.S.C. §2703(f) on April 30, 2020, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A (each an “Account”):

1. The contents of all emails and instant message communications associated with the Account from **July 1, 2011, through the present**, including stored or preserved copies of emails sent to and from the Account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

2. All records or other information regarding the identification of the Account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the Account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number) (collectively, “Account Identification Information”);

3. Source and destination addresses and header or routing information for each communication (including originating IP addresses of emails); the date, size, and length of each

communication; and any user or device identifiers linked to each communication (including cookies);

4. All records or other information stored by an individual using the Account, including address books, contact and buddy lists, calendar data, pictures, and files;

5. All device or user identifiers that have ever been linked to the Account, including but not limited to all cookies and similar technologies, unique application numbers, hardware models, operating system versions, device serial numbers, Global Unique Identifiers (“GUID”), mobile network information, telephone numbers, Media Access Control (“MAC”) addresses, and International Mobile Equipment Identities (“IMEI”);

6. All Account Identification Information (as defined above) for any accounts linked to the Account by a common email address (such as a common recovery email address), common telephone number, common means of payment (e.g., credit card number), common registration or login IP addresses (during a one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

7. The types of service utilized;

8. All records and other information concerning any record, document, or other computer file created, stored, revised, or accessed in connection with the account or by an account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers; and

9. All records pertaining to communications between the Provider and any person regarding the Account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the Special Agent listed below via United States mail, courier, or email within **14 days** of the issuance of this warrant:

Special Agent Sean Williams  
Sean.williams@tigta.treas.gov  
550 Main Street Room 5-610  
Cincinnati, OH 45202



## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 1028(a)(7) (unlawful transfer, possession, or use of a means of identification), 1028A (aggravated identity theft), and 1343 (wire fraud), as well as conspiracy to commit the foregoing offenses, those violations involving VICTOR TORRES, ADESH BISSOON, MICHAEL JOSEPH, and other unknown persons and occurring during and after July 2011, specifically, for each account or identifier listed on Attachment A (each an “Account,” and collectively “the Accounts”), information pertaining to the following matters:

1. Information relating to the identification or location of the user(s) of the Account;
2. Information relating to persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) in the commission of the criminal activity under investigation; or (ii) communicated with the account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;
3. Information relating to the Account user’s state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning related to the criminal activity under investigation;
4. Information relating to how and when the Account was accessed or used, to the geographic and chronological context of account access, use, and events relating to the crime under investigation and the account user;

5. Information relating to the theft and trafficking of personally identifiable information (PII);
6. Information relating to the identities of victims of identity theft;
7. Information relating to the use of stolen PII to commit other offenses, including but not limited to stealing or fraudulently obtaining funds through wire fraud or by filing fraudulent tax returns;
8. The identity of the person(s) who communicated with the Account about matters relating to the fraudulent scheme involving stolen PII, including records that help reveal their whereabouts;
9. All information pertaining to access to any Internal Revenue Service (“IRS”) website or service and any information obtained from the IRS or other tax-related information;
10. Evidence relating to the preparation or planning related to the criminal activities under investigation;
11. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.